Remarks/Arguments

Claims 1-7 are pending. The claims have been amended to conform with US practice.

Rejection of Claims 1-7 under 35 USC 103(a) as being unpatentable over Chaney (US 6,035,037) in view of Santis et al.

The Office Action lists pending claims 1-8, but Applicants submit that in view of the Preliminary Amendment filed on June 8, 2002, claims 1-7 are currently pending. Applicants submit that for the reasons discussed below present claims 1-7 are patentably distinguishable over the cited prior art references.

The Office Action acknowledges that Chaney fails to teach the limitation of generating the scrambling key based on a first seed value received in the smart card and a second seed value, the **second seed value being permanently stored in the smart card**. Santis is cited as supplying the missing limitations, and the Office Action alleges that Chaney and Santis may be combined to produce the claimed invention.

Applicants respectfully disagree that Santis provides the missing limitations. Santis relates to cryptosystems using a shareable functions mechanism (see Introduction, second para., and section 1.2). In that regard, Santis teaches the function sharing primitive, which includes two phases, the shadow function generation phase, and the function reconstruction phase. In the shadow function generation phase programs $\{P_1, \ldots P_l\}$ are generated in response to a randomly drawn tuple consisting of two h bit strings (pu, se), where pu is the public key and the se is the secure key (see section 3.1). In the function reconstruction phase a threshold (at least t) of partial results $P_i(\alpha)$ are created from a public input α and combined to construct a desired function (see section 3.1)

The portions of Santis cited by the Office Action relate to developing function sharing primitives for functions which are share-translateable, which is one of two conditions for function sharing (see section 4, and section 4.1). Nowhere does Santis teach or suggest generating a descrambling key using a first seed value received and a second seed value that is permanently stored in the smart card during the shadow function generation phase as alleged by the Office Action. The shadow function generation phase cited by the Office Action

computes $[s'_{i,0},\ldots,s'_{i,q-2}]$ based on input (pu, se) to the function sharing primative. Also, nowhere does Santis teach or suggest receiving data representative of a first seed value in the shared functions evaluation phase as alleged by the Office Action. In the shared functions evaluation phase a threshold (at least t) of partial results are created to calculate $y_{i,\Lambda}$ and compute $[f^{-1}{}_k(\alpha), ..]$. Nowhere do the cited portions teach or suggest the cited limitations as alleged by the Office Action. In view of the above, Applicants submit that Santis et al. fails to cure the defect of Chaney as applied to present claim 1.

Applicants further submit that nowhere does Santis or Chaney teach or suggest such a combination. Chaney relates to a system for processing a video signal using series connected smart cards. In particular, Chaney is directed to a system for providing a multiple image display, such as a picture in picture or picture outside picture, by processing a plurality of scrambled signal components that are descrambled using a plurality of smart cards coupled in series. The teachings of Santis have been discussed hereinabove. In particular, Santis is concerned with multi-agent cryptosystems, see section 7, and introduction first para. Nowhere does Chaney teach or mention the use of a multi-agent cryptographic system using shadow functions as discussed in Santis. Nowhere does the system of Chaney suggest generating a function based on multi-agent operation with a shareable functions mechanism. In view of the above, applicants submit that nowhere do Chaney or Santis teach or suggest combining the references in the manner suggested.

In view of the above, applicant respectfully submit that the combination of Chaney and Santis fail to teach or suggest all of the limitations of present claim 1, and as such, claim 1, and the claims that depend therefrom, are patentably distinguishable over the cited combination. Claim 5 recites the above-cited features in apparatus form, and as such, applicants submit that claim 5, and the claims that depend therefrom, are patentable over the cited combination for the same reasons as those discussed above.

Having fully addressed the Examiner's rejections, Applicants submit that the present application is in condition for allowance and respectfully request such action. No fee is believed due in regard to the present amendment. However, if a fee is due, please charge the fee to Deposit Account 07-0832. Should any

questions arise regarding any of the above, the Examiner is requested to contact the undersigned at 609-734-6815.

Respectfully submitted,
A. Eskicioglu, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: 4/15/04

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop No Fee Amendment, Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

4/15/04
Date

Eliza Buchalczyk